Būla funkciju sarežģītības mēri

Autors: Krišjānis Prūsis, kp08074

Darba vadītājs: Andris Ambainis, prof., Dr. dat.

Latvijas Universitāte
Datorikas fakultāte

2014. gada 12. novembrī

Funkcijas jutīgums

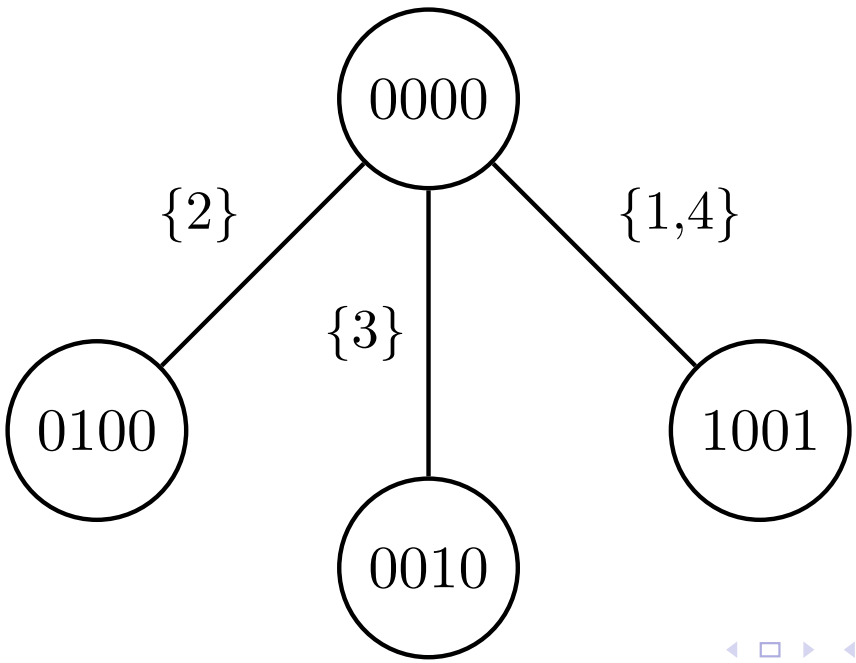
- Funkcijas jutīgums uz ievadvārdu $s(f,x)$ ir bitu skaits vārdā x, kurus nomainot, mainās funkcijas vērtība: $f(x) \neq f(x^{\{i\}})$.
- $s(f) = \max\{s(f,x) \mid x \in \{0,1\}^n\}$.
- $s_z(f) = \max\{s(f,x) \mid x \in \{0,1\}^n, f(x) = z\}$.
- Piemēram, 4 bitu vairākuma funkcijai MAJ_4
  - $s(\mathrm{MAJ}_4, 0011) = 2$,
  - $s(\mathrm{MAJ}_4, 1101) = 3$,
  - $s(\mathrm{MAJ}_4, 1111) = 0$,
  - $s_0(\mathrm{MAJ}_4) = 2$,
  - $s_1(\mathrm{MAJ}_4) = s(\mathrm{MAJ}_4) = 3$.

Funkcijas bloku jutīgums

- Funkcijas bloku jutīgums uz ievadvārdu $bs(f,x)$ ir lielākais tāds skaitlis b, ka eksistē b nešķeļošas indeksu kopas $B_1, \ldots, B_b \in [n]$, kurām $f(x) \neq f(x^{B_i})$.
- $bs(f) = \max\{bs(f,x) \mid x \in \{0,1\}^n\}$.
- $bs_z(f) = \max\{bs(f,x) \mid x \in \{0,1\}^n, f(x) = z\}$.

Bloku jutīguma piemērs

- 4 bitu sakārtotības funkcija ORD_4 ir 1 tad un tikai tad, ja ievades biti ir sakārtoti.
- Sakārtoti ir, piemēram, vārdi 0000, 0011, 1000, bet ne 1011.
- $s(\mathrm{ORD}_4) = 2$.
- $bs(\mathrm{ORD}_4) = 3$.
- Piemēram, vārdam 0000 ir 3 jutīgi bloki:



Sertifikāti

- Sertifikāts c ir tāds daļējs vērtību piekārtojums ievades pozīcijām $c : S \to \{0,1\}, S \subseteq [n]$, ka tas nosaka funkcijas vērtību.
- Sertifikātu sarežģītība uz ievadvārdu $C(f,x)$ ir garums īsākajam sertifikātam, kuram x atbilst.
- Ekvivalenti $C(f,x)$ ir mazākais x bitu skaits, kuru vērtība jāzina, lai varētu viennozīmīgi pateikt funkcijas vērtību.
- $C(f) = \max\{C(f,x) \mid x \in \{0,1\}^n\}$.
- z-sertifikāts nosaka funkcijas vērtību z.
- $C_z(f) = \max\{C(f,x) \mid x \in \{0,1\}^n, f(x) = z\}$.

Sertifikātu piemērs

- 4 bitu vairākuma funkcijai MAJ_4
  - 0-sertifikāti ir, piemēram, $00**$, $0*00$;
  - 1-sertifikāti ir, piemēram, $*111$, 1111;
  - sertifikāti nav, piemēram, $0***$, $10**$;
  - $C_0(f) = 2$;
  - $C_1(f) = C(f) = 3$.

Zināmās sakarības

- Bloku jutīgumam ir zināmas polinomiālas saistības ar daudziem citiem sarežģītības mēriem:

	$bs(f)$	$C(f)$	$D(f)$	$\deg(f)$
$bs(f)$	–	$O(C(f))$	$O(D(f))$	$O(\deg(f)^2)$
$C(f)$	$O(bs(f)^2)$	–	$O(D(f))$	$O(\deg(f)^3)$
$D(f)$	$O(bs(f)^3)$	$O(C(f)^2)$	–	$O(\deg(f)^3)$
$\deg(f)$	$O(bs(f)^3)$	$O(C(f)^2)$	$O(D(f))$	–

Aplūkotā problēma

- *Sensitivity conjecture* – arī jutīgums ir polinomiāli saistīts ar šiem mēriem.
- Tradicionāli tiek aplūkota saistība starp $s(\hat{f})$ un $bs(\hat{f})$.
- Labākie zināmie ierobežojumi – eksponenciāli.
- Labākās zināmās konstrukcijas – kvadrātiskas.

Labākie ierobežojumi

- Ilgu laiku labākais bija Kenyon un Kutin 2004. gada rezultāts:

$$bs(f) \leqslant \frac{e}{\sqrt{2\pi}} e^{s(f)} \sqrt{s(f)}.$$

- Ambainis, Bavarian, Gao, Mao, Sun un Zuo to nesen uzlaboja:

$$bs(f) \leqslant 2^{s(f)-1} s(f).$$

Labākās konstrukcijas

- Ilgu laiku labākā bija Rubinstein 1995. gada konstrukcija:

$$bs(f) = \frac{1}{2}s(f)^2.$$

- Virza to nedaudz uzlaboja:

$$bs(f) = \frac{1}{2}s(f)^2 + \frac{1}{2}s(f).$$

- Ambainis un Sun to uzlaboja vairāk:

$$bs(f) = \frac{2}{3}s(f)^2 - \frac{1}{3}s(f).$$

Rubinstein konstrukcija

- Aplūkojam funkciju g no $m = 2k$ mainīgajiem, kura ir 1 tad un tikai tad, ja izpildās viens no šāda veida sertifikātiem (piemērā $k = 5$):

$$\begin{pmatrix} 11 & 00 & 00 & 00 & 00 \\ 00 & 11 & 00 & 00 & 00 \\ 00 & 00 & 11 & 00 & 00 \\ 00 & 00 & 00 & 11 & 00 \\ 00 & 00 & 00 & 00 & 11 \end{pmatrix}.$$

- $s_0(g) = 1$, $s_1(g) = m$, $bs_0(g) = m/2$.
- Konstruējam f kā OR kompozīciju ar šo g:

$$f(x) = \bigvee_{i=1}^{m} g(x_{i,1}, \ldots, x_{i,m}).$$

- $s_0(f) = m$, $s_1(f) = m$, $bs_0(f) = m^2/2$.
- Tātad $bs(f) = \frac{1}{2}s(f)^2$.

Virzas konstrukcija

- Aplūkojam funkciju g no $m = 2k+1$ mainīgā, kura ir 1 tad un tikai tad, ja izpildās viens no šāda veida sertifikātiem (piemērā $k = 5$):

$$\begin{pmatrix} 11 & 00 & 00 & 00 & 00 & 0 \\ 00 & 11 & 00 & 00 & 00 & 0 \\ 00 & 00 & 11 & 00 & 00 & 0 \\ 00 & 00 & 00 & 11 & 00 & 0 \\ 00 & 00 & 00 & 00 & 11 & 0 \\ 00 & 00 & 00 & 00 & 00 & 1 \end{pmatrix}.$$

- $s_0(g) = 1$, $s_1(g) = m$, $bs_0(g) = k+1$.
- Konstruējam f kā OR kompozīciju ar šo g:

$$f(x) = \bigvee_{i=1}^{m} g(x_{i,1}, \ldots, x_{i,m}).$$

- $s_0(f) = m$, $s_1(f) = m$, $bs_0(f) = m^2/2 + m/2$.
- Tātad $bs(f) = \frac{1}{2}s(f)^2 + \frac{1}{2}s(f)$.

Ambaiņa un Sun konstrukcija

- Aplūkojam funkciju g no $m = 2(2k+1)$ mainīgā, kura ir 1 tad un tikai tad, ja izpildās viens no šāda veida sertifikātiem (piemērā $k = 2$):

$$\begin{pmatrix} 11 & 00 & 00 & 0* & 0* \\ 0* & 11 & 00 & 00 & 0* \\ 0* & 0* & 11 & 00 & 00 \\ 00 & 0* & 0* & 11 & 00 \\ 00 & 00 & 0* & 0* & 11 \end{pmatrix}.$$

- $s_0(g) = 1$, $s_1(g) = 3k+2$, $bs_0(g) = 2k+1$.
- Konstruējam f kā OR kompozīciju ar šo g:

$$f(x) = \bigvee_{i=1}^{3k+2} g(x_{i,1}, \ldots, x_{i,m}).$$

- $s_0(f) = 3k+2$, $s_1(f) = 3k+2$, $bs_0(f) = (3k+2)(2k+1)$.
- Tātad $bs(f) = \frac{2}{3}s(f)^2 - \frac{1}{3}s(f)$.

Konstrukciju vispārinājums

- Funkcija g ar $s_0(g) = 1$, $s_1(g) = m$, $bs_0(g) = k$.
- $f(x) = \bigOR_{i=1}^{m} g(x_{i,1}, \ldots, x_{i,n})$.
- $s_0(f) = m$, $s_1(f) = m$, $bs_0(f) = km$.
- Ambainis un Sun pierāda, ka ar šādu konstrukciju $bs(f) = \frac{2}{3}s(f)^2 - \frac{1}{3}s(f)$ ir optimāls.

Aplūkotais variants

- Funkcija g ar $s_0(g) \geqslant 2$.
- $f(x) = \bigOR_{i=1}^{s_1(g)/s_0(g)} g(x_{i,1}, \ldots, x_{i,n})$.
- Lai uzlabotu šobrītējo rezultātu, nepieciešams

$$s_1(g) < \frac{3}{2} \frac{bs_0(g)}{s_0(g)}.$$

Saistība ar sertifikātu sarežģītību

- Visām labākajām konstrukcijām $s_1(f) = C_1(f)$.
- Izvirzam hipotēzi, ka funkcijām, kas maksimizē atšķirību starp $s_0(f)$ un $bs_0(f)$ vienmēr izpildās šī sakarība.
- Kenyon un Kutin pierāda, ka

$$C_1(f) \geqslant \frac{1}{2}\frac{bs_0(f)}{s_0(f)}.$$

- Taču pie $s_1(f) = C_1(f)$ tas ļauj iegūt funkciju, kurai

$$bs(f) = 2s(f)^2.$$

- Šādu funkciju iterējot varētu iegūt virs-kvadrātisku atšķirību.

Rezultāts

- Uzlabojam Kenyon un Kutin rezultātu uz

$$C_1(\hat{f}) \geqslant \frac{3}{2}\frac{bs_0(\hat{f})}{s_0(\hat{f})} - \frac{1}{2}.$$

- Šī robeža ir asimptotiski cieša, jo OR no $s_0(\hat{f})$ Ambaiņa un Sun konstrukcijā izmantotajām funkcijām g ļauj patvaļīgam $s_0(\hat{f})$ iegūt funkciju, kurai

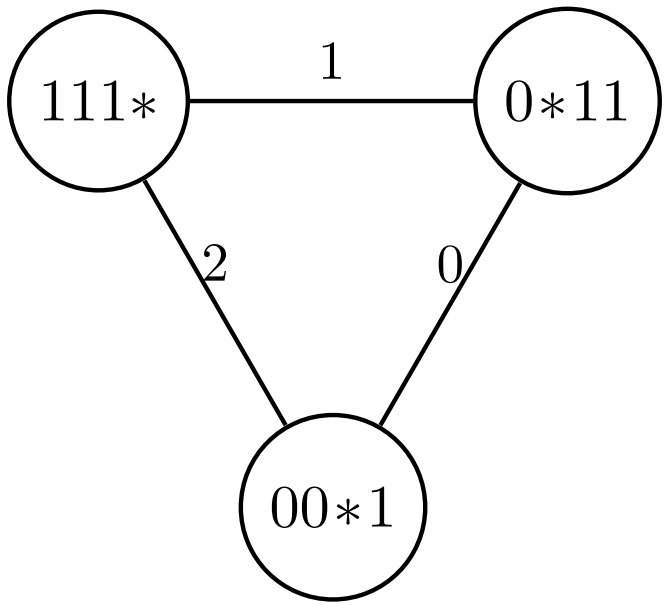
$$C_1(\hat{f}) = \frac{3}{2}\frac{bs_0(\hat{f})}{s_0(\hat{f})} + \frac{1}{2}.$$

Pierādījums

- Nezaudējot vispārīgumu varam pieņemt, ka 0-ievade, kas sasniedz $bs_0(f)$, ir visas nulles – 0^n.
- Katrs vārds $\{0^n\}^{B_i}$ atbilst citam minimālajam 1-sertifikātam $c_1, \ldots, c_{bs_0(f)}$.

Sertifikātu pretrunu grafs

- Izveidojam $bs_0(f)$ virsotņu pilnu grafu G – katra virsotne atbilst kādam c_i.
- Katrai šķautnei piekārtojam svaru – pretrunu skaitu starp atbilstošajiem sertifikātiem.
- Piemērs ar dažiem 1-sertifikātiem sakārtotības funkcijai ORD_4:



Grafa svars

- Par grafa svaru $w(G)$ sauksim tā šķautņu svaru summu.
- Parādīsim, ka

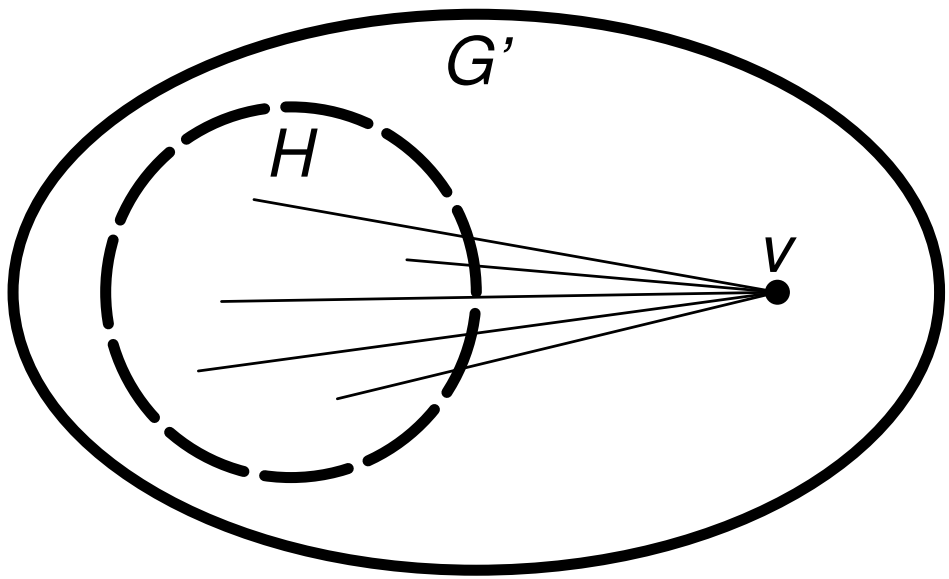
$$w(G) \geqslant \frac{3}{2}\frac{bs_0(f)^2}{s_0(f)} - \frac{3}{2}bs_0(f).$$

Indukcija pār apakšgrafiem

- Aplūkojam inducētu apakšgrafu $G' = (V', E')$. Apzīmējam $|V'| = m$.
- Parādīsim, ka
$$w(G') \geqslant \frac{3}{2}\frac{m^2}{s_0(f)} - \frac{3}{2}m.$$
- Bāze: $m \leqslant s_0(f)$. Tad
$$\frac{3}{2}\frac{m^2}{s_0(f)} - \frac{3}{2}m \leqslant 0,$$
bet $w(G') \geqslant 0$.

Indukcijas solis

- $m > s_0(f)$, visiem mazākiem apakšgrafiem īpašība jau pierādīta.
- Atrodam šī apakšgrafa $s_0(f)$ virsotņu inducēto apakšgrafu ar mazāko svaru. Apzīmējam šo grafu ar H.
- Parādīsim, ka katram sertifikātam $v \in G' \setminus H$ ar visiem H sertifikātiem kopā ir vismaz 3 pretrunas.

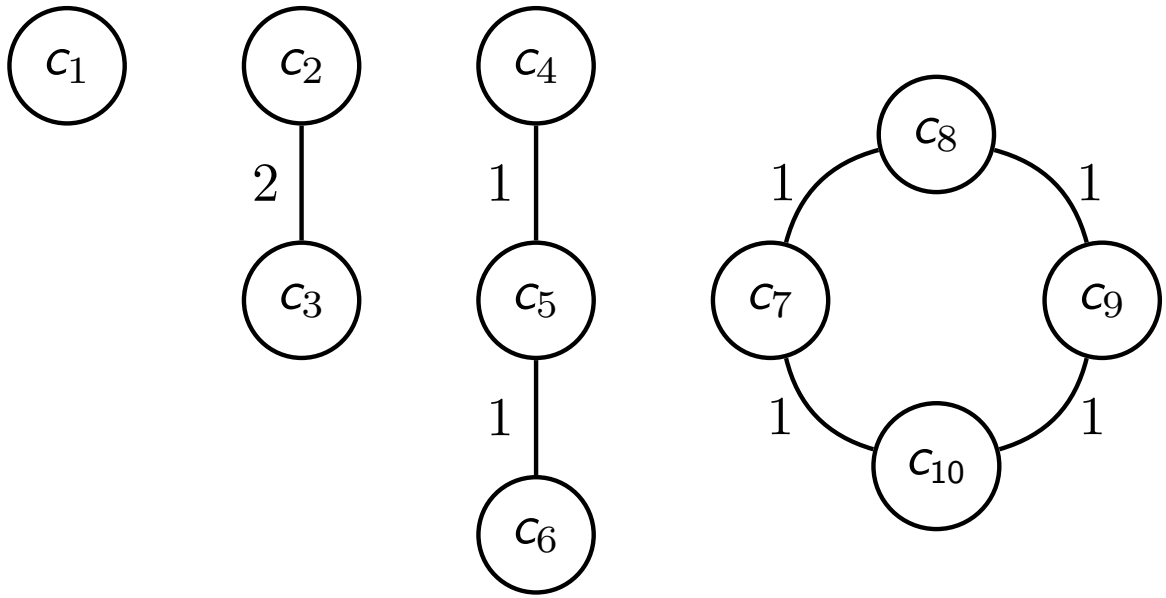


Virsotne ar < 3 pretrunām

- Pieņemam pretējo, eksistē $v \in G' \setminus H$, kurai ar H ir ne vairāk kā 2 pretrunas.
- Tad Aplūkojam G' induceto apakšgrafu $H' = H \cup \{v\}$. Tajā būs $s_0(f) + 1$ virsotne un ne vairāk kā $w(H) + 2$ pretrunas.
- Ja eksistētu $u \in H'$, kuram H' iekšienē ir vismaz 3 pretrunas, tad $H' \setminus \{u\}$ būtu $s_0(f)$ izmēra apakšgrafs ar mazāku svaru par $w(H)$. Tātad tāds neeksistē.
- Līdz ar to H' iekšienē katram sertifikātam ar pārējiem ir ne vairāk kā 2 pretrunas.

Sertifikātu grafi ar maz pretrunām

- Sertifikātu pretrunu grafs, kur katram ar pārējiem ir ne vairāk kā 2 pretrunas, var sastāvēt tikai no dažu veidu komponentēm ar ne-nulles šķautnēm:



- Darbā pierādīts, ka funkcijai ar šādu 1-sertifikātu grafu 0-jutīgums ir vismaz tā virsotņu skaits..
- H' ir $s_0(f)+1$ virsotnes, līdz ar to mēs iegūtu $s_0(f) \geqslant s_0(f)+1$ – pretrunu.

Indukcijas pāreja

- Grafā $G' \setminus H$ būs $m - s_0(f)$ sertifikāti, tātad pēc indukcijas vismaz šāds skaits pretrunu:

$$\frac{3}{2}\frac{(m - s_0(f))^2}{s_0(f)} - \frac{3}{2}(m - s_0(f)).$$

- Pēc iepriekš pierādītā starp katru $v \in G' \setminus H$ un H ir vēl vismaz 3 pretrunas, tātad kopā ir vēl $3(m - s_0(f))$ šādu pretrunu.

- Tātad kopā grafā G' būs vismaz nepieciešamais skaits pretrunu:

$$\frac{3}{2}\frac{(m - s_0(f))^2}{s_0(f)} - \frac{3}{2}(m - s_0(f)) + 3(m - s_0(f)) =$$

$$\frac{3}{2}\frac{m^2}{s_0(f)} - \frac{3}{2}m.$$

Pierādītais rezultāts

- Ņemot kā G' pašu G iegūstam meklēto:

$$w(G) \geqslant \frac{3}{2}\frac{bs_0(f)^2}{s_0(f)} - \frac{3}{2}bs_0(f).$$

- Katra pretruna atbilst nullei vienā no c_i. Sertifikātu kopā ir $bs_0(f)$, tātad vismaz vienam no tiem ir vismaz

$$\frac{3}{2}\frac{bs_0(f)}{s_0(f)} - \frac{3}{2}$$

nuļļu. Katram no tiem vēl ir vismaz viens vieninieks, līdz ar to

$$C_1(f) \geqslant \frac{3}{2}\frac{bs_0(f)}{s_0(f)} - \frac{1}{2}.$$

Turpmākais darbs

- Turpmāk varētu pētīt sakarību starp $C_1(f)$ un $s_1(f)$. Tos saista šāda sakarība:

$$C_1(f) \leqslant 2^{s_0(f)-1} s_1(f) - (s_0(f) - 1).$$

- No otras puses, labākajām zināmajām funkcijām, kas šo atšķirību maksimizē, $C_1(f) = O(s_0(f)s_1(f))$.

- Jau pie $s_0(f) = 2$ nav zināmas funkcijas, kas sasniedz šo robežu $C_1(f) \leqslant 2s_1(f) - 1$.

Paldies par uzmanību